Transportation Security Administration

NOTE: This Technical Advisory describes a matter which may impact your product.

TWIC Technical Advisory TA-2014-TWIC001-V1.0

CHANGE OF CERTIFICATE AUTHORITY SERVICE PROVIDER

Introduction

This Technical Advisory details the change from the current Certificate Authority (CA) service provider to a new CA service provider.

Background and Definition

Attachment A of this Technical Advisory details the format of each CA service provider certificate.

Problem Statement

The TWIC program will soon begin issuing cards from a new Card Production platform. This new platform employs a new CA service provider. As a result, new ROOT and subordinate CA certificates must be introduced. In addition a new limited set of Content Signing certificates shall be issued for use across all TWIC cards issued under the new Card Production platform.

Description of New or Unique Process

The TWIC program has made every effort to maintain the same CA certificate structure as used under the current CA service provider. However, values in one or more X.509 fields will differ (e.g. URL addresses). Attachment A provides a detailed certificate profile for each certificate type to be issued under the new CA service provider.

Use of New or Unique Process

TWIC reader vendors are encouraged to incorporate the new TWIC ROOT and subordinate CA certificates into their implementations as soon as practical. TWIC vendors are discouraged from caching the Content Signing certificate as the new CA service provider shall populate for each TWIC card one of a limited set of Content Signing certificates (refer to A.7 and in particular the format of the Subject Distinguished Name field).

The TWIC program recognizes that not all implementations will be able to decode the PKCS#7 certificate file to extract the DER binary encoded certificate(s). Therefore, TWIC will make available the DER Binary encoded form of the ROOT and subordinate CA certificates at the following location: http://www.tsa.gov/stakeholders/reader-qualified-technology-list-qtl.

Design Features of New or Unique Process

The new CA service provider shall use new URL and LDAP addresses. Additional Object Identifiers (OIDs) have been used to enhance interoperability. A new set of Certificate Revocation Lists (CRLs) shall be provided. The current CRLs under the current CA service provider shall be maintained until no longer required.

Comments

Questions on this Technical Advisory should be addressed to the TSA TWIC PMO TWIC Reader Hardware and Card Application Specification Project Editor, Gerald.Smith@associates.dhs.gov .

Subject References

(Clarified) TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, May 2012.

Keywords

TWIC
Certificate Authority
Certificate Revocation List

Standard Details

Refer to Section 2 *References* in the Subject Reference document.

Specifications or Special Provision

(Clarified) TWIC Reader Hardware and Card Application Specification, Version 1.1 Amendment 1, May 2012.

Supersedes Dates

There is no previous Technical Advisory issued that addresses this unique change.

This Technical Advisory shall be active until further notice.

Obtain more Information

More technical information on TWIC can be obtained at the web address of:

http://www.tsa.gov/stakeholders/reader-qualified-technology-list-qtl

END

Attachment A

This attachment details the profile formats for each certificate issued under the new Certificate Authority Service Provider. [Source: Version 1.3 of the TWIC Certificate Policy].

A.1 TWIC Root CA Self-Signed Certificate

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC ROOT, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 25-years (example is 17)
Subject Distinguished Name	cn=TWIC ROOT, ou= TSA Certification Authorities o = U.S. Government, c= US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical = no; KeyID = Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC Root CA's public key information)
Subject key identifier	critical = no; Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC Root CA public key information)
Key usage	critical = **yes**; Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Enhanced key usage	
Private key usage period	
Certificate policies	Critical = no; Policy Identifier=1.3.6.1.4.1.29138.2.1 anyPolicy (2.5.29.32.0)
Policy Mapping	
Subject Alternative Name	
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	critical= **yes**; Subject Type = CA; path length constraint = None
Name Constraints	
Policy Constraints	
Authority Information Access	
CRL Distribution Points	
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

A.2 TWIC Subordinate CA Certificate (CA 1 illustrated)

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC ROOT, ou= TSA Certification Authorities o = U.S. Government, c=US
Validity Period	10 years from date of issue in UTCT format
Subject Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c=US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical = no; keyID = Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC Root CA's public key information)
Subject key identifier	critical = no; Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC CA 1 public key information)
Key usage	critical = **yes**; Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Enhanced key usage	
Private key usage period	
Certificate policies	critical =no; Policy Identifier=1.3.6.1.4.1.29138.2.1.3 Policy Identifier=1.3.6.1.4.1.29138.2.1.3.5 Policy Identifier=1.3.6.1.4.1.29138.2.1.3.6 Policy Identifier=1.3.6.1.4.1.29138.2.1.3.13 Policy Identifier=1.3.6.1.4.1.29138.2.1.3.17 Policy Identifier=2.16.840.1.101.3.6.7
Policy Mapping	
Subject Alternative Name	
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	critical= **yes**; Subject Type = CA; path length constraint = None
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICRootCA.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20ROOT,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
Subject Information Access	
CRL Distribution Points[1]	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TWICRoot.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20ROOT,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

[1] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.3 TWIC Individual Digital Signature Certificate

Field	Identity Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 5 years from date of issue
Subject Distinguished Name	cn = Full Name, ou = TWIC, o = TSA, c = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier[2]	critical =no; keyID = octet string of 20 bytes
Subject key identifier[3]	critical =no; octet string of 20 bytes
Key usage	critical = **yes**; digitalSignature, nonrepudiation (c0)
Enhanced key usage	critical = no; Any Purpose (2.5.29.37.0) Client Authentication (1.3.6.1.5.5.7.3.2)
Private key usage period	
Certificate policies	critical = no; Policy Identifier=1.3.6.1.4.1.29138.2.1.3.5 (id-TWIC-DigitalSignature-policy)
Policy Mapping	
subject Alternative Name	critical = no; contains RFC822 e-mail address (only if provided by Individual)
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points[4]	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

[2] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[3] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[4] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.4 (TWIC) PIV Individual Administrative Key Management Certificate

Field	Encryption Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 5 years from date of issue
Subject Distinguished Name	cn = Full Name, ou = TWIC, o = TSA, c = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier[5]	critical =no; keyID = octet string of 20 bytes
Subject key identifier[6]	critical =no; octet string of 20 bytes
Key usage	critical = **yes**; Key Encipherment (20)
Enhanced key usage[7]	critical = no; Any Purpose (2.5.29.37.0) Secure Email (1.3.6.1.5.5.7.3.4) Encrypting File System (1.3.6.1.4.1.311.10.3.4)[11]
Private key usage period	
Certificate policies	critical = no; Policy Identifier=1.3.6.1.4.1.29138.2.1.3.6 (id-TWIC-KeyManagement-policy)
Policy Mapping	
subject Alternative Name	critical = no; not present OR RFC822 e-mail address if provided by Individual
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points[8]	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

[5] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the signing CA's public key information.

[6] The value of this field is the 20 byte SHA-1 hash of the binary DER encoding of the subject's public key information.

[7] Microsoft Encrypted File System MS-EFS {1 3 6 1 4 1 311 10 3 4}

[8] The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and crlIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

A.5 (TWIC) PIV User Authentication Certificate

Field	Identity Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 5 years from date of issue
Subject Distinguished Name	cn = Full Name, ou = TWIC, o = TSA, c = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical =no; keyID = octet string of 20 bytes
Subject key identifier	critical =no; octet string of 20 bytes
Key usage	critical = **yes**; Digital Signature (80)
Enhanced key usage	critical = no; Any Purpose (2.5.29.37.0) Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Private key usage period	
Certificate policies	critical = no; Policy Identifier=1.3.6.1.4.1.29138.2.1.3.13 (id-TWIC-authentication-policy)
Policy Mapping	
subject Alternative Name	critical = no; not present OR RFC822 e-mail address if provided by Individual, Other Name: 25 byte FASC-N value under OID 1.3.6.1.4.1.29138.6.6, Other Name: AppID as email of ABCDEFGH@twicprogram.tsa.dhs.gov (where 8 CAPS are the Application ID) or ["T" concatenated with a variable number of digits] @ twicprogram.tsa.dhs.gov
twic-interim	critical = no; 01 01 00 (Background check begun) (1.3.6.1.4.1.29138.6.9.1)
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

A.6 (TWIC) PIV Card Authentication Certificate

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 5 years from date of issue
Subject Distinguished Name	SERIAL NUMBER = FASC-N (50 characters), ou = TWIC, o = TSA, c = US
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical =no; keyID = octet string of 20 bytes
Subject key identifier	critical =no; octet string of 20 bytes
Key usage	critical = **yes**; Digital Signature (80)
Enhanced key usage	critical = yes; Unknown Key Usage (1.3.6.1.4.1.29138.6.8) (id-TWIC-cardAuth)
Private key usage period	
Certificate policies	critical = no; Policy Identifier=1.3.6.1.4.1.29138.2.1.3.17 (id-TWIC-CardAuthentication-policy)
Policy Mapping	
subject Alternative Name	critical = no;, Other Name: 25 byte FASC-N value under OID 1.3.6.1.4.1.29138.6.6
Twic-interim	critical = no; 01 01 00 (Background check begun) (1.3.6.1.4.1.29138.6.9.1)
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Extensions	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

A.7 TWIC/PIV Content Signing Certificate (Common)

Field	Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Signature Hash Algorithm	sha-1
Issuer Distinguished Name	cn=TWIC CA 1, ou= TSA Certification Authorities o = U.S. Government, c= US
Validity Period	Up to 8 years from date of issue in UTCT format
Subject Distinguished Name	cn = TWIC-Content-Signing-YYYY-nnn, ou = TWIC, o = TSA, c = US (where YYYY is a year and nnn is three numeric digits)
Subject Public Key Information	2048 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	
Subject Unique Identifier	
Issuer's Signature	sha-1WithRSAEncryption
Extensions	
Authority key identifier	critical = no; keyID = Octet String (20 byte SHA-1 hash of the binary DER encoding of the Root CA's public key information)
Subject key identifier	critical = no; Octet String (20 byte SHA-1 hash of the binary DER encoding of the subject's public key information)
Key usage	critical = **yes**; Digital Signature (80)
Enhanced key usage	PIV content signing OID 2.16.840.1.101.3.6.7, TWIC content signing OID 1.3.6.1.4.1.29138.6.7.
Private key usage period	critical = no; 36 byte value of UTC time (not before / not after) DEPRECATED
Certificate policies	critical =no; Policy Identifier=2.16.840.1.101.3.6.7 (id-PIV-content-signing) , Policy Qualifier Info: [1] Policy Qualifier Id=CPS, Qualifier: 1.2.3.4.5 ; [2] Policy Qualifier Id=User Notice Qualifier: Information Not Available
Policy Mapping	
Subject Alternative Name	
Issuer Alternative Name	
Subject Directory Attributes	
Basic Constraints	
Name Constraints	
Policy Constraints	
Authority Information Access	critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: http://twicaia-twic.tsa.dhs.gov/AIA/CertsIssuedToTWICCA1.p7c critical = no; Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2); Alternative Name URL: ldap://twicaia-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?cACertificate;binary
CRL Distribution Points	critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=http://twiccrl-twic.tsa.dhs.gov/CRLs/TIMCA1.crl critical = no; always present, CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://twiccrl-twic.tsa.dhs.gov/cn=TWIC%20CA%201,ou=TSA%20Certification%20Authorities,o=U.S.%20Government,c=US?certificateRevocationList;binary
Properties	
Thumbprint Algorithm	sha-1
Thumbprint	20 byte Value

A.8 TWIC Root CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn=TWIC ROOT, ou= TSA Certification Authorities o = U.S. Government, c= US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 48 Hours
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC Root CA
CRL entry extensions	
Invalidity Date	present when received
Reason Code	Present if Reason is not Unspecified

A.9 TWIC Subordinate CA CRL

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	Sha-1WithRSAEncryption
Issuer Distinguished Name	cn=TWIC ROOT, ou= TSA Certification Authorities o = U.S. Government, c= US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 48 hours
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the TWIC CA “x” public key information)
CRL entry extensions	
Invalidity Date	present when received
Reason Code	Present if Reason is not Unspecified